



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-25

December 15, 2003

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the Department of Homeland Security Information Analysis Infrastructure Protection Directorate Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between November 11 and November 26, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3am Labs Ltd. ¹	Windows	Remotely Anywhere Enterprise Edition, Personal Edition, Server Edition, Server Edition 5.10.416	A Cross-Site Scripting vulnerability exists in the 'autologon.html' page due to insufficient filtering of HTML, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Remotely Anywhere Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹ SecurityTracker Alert, 1008310, November 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alabanza ²	Multiple	AlaCart 1.0	A vulnerability exists during the authentication process when handling username and password data, which could let a remote malicious user inject SQL commands to obtain administrative access.	No workaround or patch available at time of publishing.	AlaCart Administration Authentication Bypass	High	Bug discussed in newsgroups and websites. Exploit has been published.
Alan Ward ³	Multiple	A-Cart 2.0, PRO 2.0	A Cross-Site Scripting vulnerability exists in the 'register.asp' script due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	A-Cart Register.ASP Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Amaze soft ⁴	Windows	FlashGet 0.9-0.96, 1.0-1.2	A vulnerability exists because dial-up user credentials are stored in plain text in a registry that is in a location readable by all users, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FlashGet Insecure Dialup Credential Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Foundation ⁵	Unix	Gregory Trubetskoy mod_python 2.7-2.7.8, 3.0-3.0.3	A remote Denial of Service vulnerability exists when a malicious user submits a malformed query.	Upgrade available at: http://httpd.apache.org/modules/python-download.cgi	Apache mod_python Module Remote Denial of Service CVE Name: CAN-2003-0973	Low	Bug discussed in newsgroups and websites.
Apple ⁶	MacOS X	Apple Share IP 5.0-5.0.3, 6.1-6.3.1	A remote Denial of Service vulnerability exists when a malicious user invokes the 'RMD' command in a specific manner.	Upgrade available at: http://www.apple.com/apple/shareip/	AppleShare IP FTP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple ⁷ <i>Patch now available⁸</i>	Multiple	Safari 1.0, 1.1	A vulnerability exists due to an error when handling URLs, which could let a malicious user obtain sensitive information.	<i>Patch available at: http://download.info.apple.com/Mac_OS_X/061-0935.20031205.cft4r/2Z/SecurityUpd2003-12-05Jag.dmg</i>	Safari Web Browser Null Character Cookie Stealing CVE Name: CAN-2003-0975	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

² Securiteam, November 30, 2003.

³ Bugtraq, December 4, 2003.

⁴ Bugtraq, December 10, 2003.

⁵ Secunia Advisory, SA10325, December 1, 2003.

⁶ Bugtraq, December 5, 2003.

⁷ Secunia Advisory, SA10252, November 25, 2003.

⁸ Apple Security Update, December 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Applied Watch Technologies, Inc. ⁹	Unix	Applied Watch Command Center 1.0	Two vulnerabilities exist: a vulnerability exists due to a failure to authenticate certain messages, which could let a remote malicious user add new accounts to the system; and a vulnerability exists because a specially crafted message can be submitted to add a custom intrusion detection rule to all sensor nodes on the managed network, which could let a remote malicious user modify detection rules.	Update available at: https://my.appliedwatch.com	Applied Watch Command Center Authentication Bypass & Detection Rule Modification CVE Name: CAN-2003-0974	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Aprelium Technologies ¹⁰	Unix	Abyss Web Server 1.0, 1.0.3, 1.0.7, 1.1.2, 1.1.4, 1.1.6 Beta	A vulnerability exists because it is possible to access password protected directories on a FAT32 file system without supplying a valid password, which could let a malicious user bypass authentication.	Upgrades available at: http://www.aprelum.com/abysws/download.php	Abyss Web Server Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Baldor ¹¹	Unix	detecttr.c	A format string vulnerability exists due to the erroneous usage of the syslog() function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Traceroute Detection Security Tool Remote Format String	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Bens Scripts ¹²	Unix	Guestbook 1.0	A vulnerability exists in the comment field due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Guestbook Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.

⁹ Bugtraq Security Systems, Incorporated, November 28, 2003.

¹⁰ Secunia Advisory, SA10386, December 8, 2003.

¹¹ Secure Network Operations, Inc. Advisory, SRT2003, November 27, 2003.

¹² SecurityFocus, December 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CalaCode ¹³	Windows, Unix	@mail Webmail System 3.52 Demo	Multiple vulnerabilities exist: a vulnerability exists in the 'showmail.pl' script due to a failure to validate the user-supplied 'Folder' parameter, which could let a remote malicious user access another user's mailbox; a vulnerability exists in the 'atmail.pl,' 'search.pl,' and 'reademail.pl' scripts due to insufficient input validation, which could let a remote malicious user execute arbitrary code; a vulnerability exists because a remote malicious user can modify a mailbox name cookie to obtain access to a target user's mailbox if the target user has an active session at the time; and a vulnerability exists in the 'showmail.pl' script due to a failure to filter HTML code from user-supplied requests, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	@mail Webmail System Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Cezary M Kruk ¹⁴	Unix	Cdwrite 1.3	A vulnerability exists due to insecure creation of temporary files, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Cdwrite Insecure Temporary File	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems ¹⁵	Multiple	Cisco 80-7111-01 for the UNITY-SVRX255-1A, UNITY-SVRX255-2A,	Multiple vulnerabilities exist in the Cisco Unity running on IBM servers because they contain default user accounts and default IP addresses, which could let a malicious user obtain unauthorized access.	Workaround available at: http://www.cisco.com/warp/public/707/cisco-sa-20031210-unity.shtml	Cisco Unity Default User Accounts & IP Addresses	Medium	Bug discussed in newsgroups and websites.
Cisco Systems ¹⁶	Multiple	IOS 12.2 (8)JA, IOS 12.2 (11)JA1, 12.2 (11)JA	An information disclosure vulnerability exists if the 'snmp-server enable traps wlan-wep' command has been set because static WEP keys are sent to the SNMP server in clear text when a key is changed or the device is rebooted, which could let a remote malicious user view the static Wired Equivalent Privacy (WEP) key.	Workaround and upgrade available at: http://www.securityfocus.com/advisories/6124	Aironet Access Point Wired Equivalent Privacy Key Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹³ S-Quadra Advisory, December 9, 2003.

¹⁴ Secunia Advisory, SA10392, December 9, 2003.

¹⁵ Cisco Security Advisory, 47186, December 10, 2003.

¹⁶ Cisco Security Advisory, cisco-sa-20031202, December 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ¹⁷	Multiple	Application & Content Networking Software 4.0.3, 4.1.1, 4.1.3, 4.2, 4.2.7, 4.2.9, 5.0, 5.0.1, 5.0.3, Content Distribution Manager 4630, 4.0, 4.1, 4650, 4.0, 4.1, 4670, Content Engine 507, 2.2.0, 3.1, 4.0, 4.1, 560, 2.2.0, 3.1, 4.0, 4.1, 590, 2.2.0, Cisco Content Engine 590, 2.2.0, 3.1, 4.0, 4.1, 7320, 2.2.0, 3.1, 4.0, 4.1, Content Engine Module for Cisco Router 2600 Series, 3600 Series, 3700 Series, Content Router 4430, 4.0, 4.1, 4450	A buffer overflow vulnerability exists in the ACNS authentication libraries, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	This issue has been addressed in the 4.2.11 and 5.0.5 releases of ACNS. The 5.1 releases are also not vulnerable to this issue. Upgrades available at: http://www.cisco.com/warp/public/707/cisco-sa-20031210-ACNS-auth.shtml	Cisco ACNS Authentication Library Remote Buffer Overflow	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

¹⁷ Cisco Security Advisory, 47184 , December 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Com-mandO Software ¹⁸	Unix	Free Scripts Visitor Book LE	Multiple input validation vulnerabilities exist: a vulnerability exists if the '\$mailuser' parameter is 1 because it is possible to inject mail headers using line breaks through the e-mail address, which could let a remote malicious user alter mail and send SPAM e-mails; a remote Denial of Service vulnerability exists when a malicious user submits entries with a large number of line breaks; a Cross-Site Scripting vulnerability exists in 'visitorbook.pl' due to insufficient verification of the 'do' parameter, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because responses are trusted from reverse DNS lookups, which could let a malicious user alter information.	No workaround or patch available at time of publishing.	Multiple VisitorBook Input Validation Vulnerabilities CVE Names: CAN-2003-0979 , CAN-2003-0980 , CAN-2003-0981	Low/ Medium/ High Low if a DoS; Medium if information can be altered; and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required.
CutePHP Team ¹⁹	Unix	CuteNews 1.3	An information disclosure vulnerability exists in the 'index.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CuteNews 'index.php' Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a roof of Concept exploit has been published.
Easy Software Products ^{20, 21, 22} <i>Turbo Linux issues advisory</i> ²³	Unix	CUPS 1.0.4-8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.18	A vulnerability exists because a remote malicious user can access the CUPS Internet Printing Protocol (IPP) port (on TCP port 631, by default) and cause the target daemon to enter a busy loop and consume excessive CPU resources.	<u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/ <u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php <u>RedHat:</u> ftp://updates.redhat.com/ <u>TurboLinux:</u> ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/	Cups Internet Printing Protocol Remote Denial of Service CVE Name: CAN-2003-0788	Low	Bug discussed in newsgroups and websites.

¹⁸ Westpoint Security Advisory, December 10, 2003.

¹⁹ Bugtraq, November 30, 2003.

²⁰ Red Hat Security Advisory, RHSA-2003:275-01, November 3, 2003.

²¹ Mandrake Linux Security Update Advisory, MDKSA-2003:104, November 6, 2003.

²² Conectiva Linux Security Announcement, CLA-2003:779, November 7, 2003.

²³ Turbolinux Security Advisory, TLSA-2003-63, November 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Eric Raymond ^{24, 25, 26} <i>Turbo Linux issues advisory</i> ²⁷	Unix	Fetchmail 5.9.0, 6.2.4	A Denial of Service vulnerability exists when a malicious user submits a specially crafted e-mail message. Execution of arbitrary code may also be possible	<u>Immunix:</u> http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/ <u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php <u>Slackware:</u> Ftp://ftp.slackware.com/pub/slackware/ <u>TurboLinux:</u> ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/	Fetchmail Remote Denial of Service CVE Name: CAN-2003-0792	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
EZnet-work ²⁸	Windows	eZ 3.5 .0	A buffer overflow vulnerability exists in 'eZnet.exe' when handling HTTP requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	EZMeeting 'EZNet.EXE' Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
EZnet-work ²⁹	Windows	EZphoto-share 1.0, 1.1	Two vulnerabilities exist due to boundary errors in 'ezphoto.exe' when receiving data on port 10101/tcp, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple EZPhotoShare Memory Corruption Vulnerabilities	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Ferry Boender ³⁰	Unix	PieterPost 0.10.6	A vulnerability exists due to insufficient authentication, which could let an unauthorized remote malicious user obtain access as a 'virtual' user.	Update available at: http://todsah.nihilist.nl/data/development/projects/pieterpost/files/pieterpost-0.10.7.tar.gz	PieterPost Unauthorized E-mail Account Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Fuzzy Monkey ³¹	Multiple	My Photo Gallery 3.1, 3.2, 3.4-3.7	A vulnerability exists due to insufficient authentication, which could let an unauthorized malicious user obtain access.	Upgrades available at: http://www.fuzzymonkey.org/files/myphotogallery-3.8.tar.gz	My Photo Gallery Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
FVWM ³²	Multiple	FVWM 2.4.17 FVWM 2.5.8	A vulnerability exists in the 'fvwm-menu-directory' component due to insufficient sanitization, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	FVWM fvwm-menu-directory	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

²⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:101, October 16, 2003.

²⁵ Immunix Secured OS Security Advisory, IMNX-2003-7+-023-01, October 20, 2003.

²⁶ Slackware Security Bulletin, SSA:2003-300-02, October 27, 2003.

²⁷ Turbolinux Security Advisory, TLSA-2003-61, November 28, 2003.

²⁸ Bugtraq, December 7, 2003.

²⁹ Secunia Advisory, SA10350, December 4, 2003.

³⁰ Bugtraq, November 29, 2003.

³¹ SecurityFocus, December 8, 2003.

³² SecurityFocus, December 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU ³³	Unix	XBoard 4.2.5, 4.2.6	A vulnerability exists in the 'pxboard' script due to insecure temporary file creation, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://ftp.gnu.org/gnu/xboard/xboard-4.2.7.tar.gz	PXBoard Script Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites.
GNU ^{34, 35}	Unix	CVS 1.10.7, 1.10.8, 1.11-1.11.6	A vulnerability exists due to a failure to detect attempts to create files and directories, which could let a malicious user create arbitrary folders and possibly files in the root of the host's file system.	CVS: http://ccvs.cvshome.org/servlets/ProjectDownloadList?action=download&dlID=384 Slackware: ftp://ftp.slackware.com/pub/slackware/	CVS Malformed Request CVE Name: CAN-2003-0977	Medium	Bug discussed in newsgroups and websites.
GNU ^{36, 37}	Unix	GNU Privacy Guard 1.2-1.2.3, 1.3.3	A format string vulnerability exists in the HKP (HTTP Keyserver Protocol) interface used for retrieval of public keys from HKP key servers, which could let a remote malicious user execute arbitrary code.	The vendor has released a fixed development version (1.3.4) and has issued a fix for the 1.2 branch, available via CVS. SuSE: ftp://ftp.suse.com/pub/suse/	GnuPG Format String	High	Bug discussed in newsgroups and websites.
GNU ^{38, 39}	Unix	screen 3.9.4, 3.9.8-3.9.11	A buffer overflow vulnerability exists in 'ansi.c' due to an integer error, which could let a malicious user execute arbitrary code.	Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release	GNU Screen Integer Overflow CVE Name: CAN-2003-0972	High	Bug discussed in newsgroups and websites.
GNU ^{40, 41, 42, 43}	Unix	GNU Privacy Guard 1.0.2, 1.0.3, 1.0.3 b, 1.0.4-1.0.7, 1.2-1.2.3	A vulnerability exists in the implementation of ElGamal signing keys, which could let a remote malicious user compromise private keys. <i>Note: The vendor reports that ElGamal encrypt-only keys (type 16) are not affected.</i>	Patch available at: http://lists.gnupg.org/pipermail/gnupg-users/2003-November/020771.html Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/	GnuPG ElGamal Signing Key Private Key Compromise CVE Name: CAN-2003-0971	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett Packard Company ⁴⁴	Unix	HP-UX 11.0 4, 11.0, 11.11	A vulnerability exists because the shar utility creates temporary files with predictable names, which could let a malicious user obtain elevated privileges.	Patches available at: http://itrc.hp.com	HP-UX Shar Utility Predictable Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

³³ SecurityTracker Alert, 1008375, December 4, 2003.

³⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:112-1, December 10, 2003.

³⁵ Slackware Security Advisory, SSA:2003-345-01, December 12, 2003.

³⁶ S-Quadra Advisory, December 3, 2003.

³⁷ SuSE Security Announcement, SuSE-SA:2003:048, December 3, 2003.

³⁸ OpenPKG Security Advisory, OpenPKG-SA-2003.050, November 28, 2003.

³⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:113, December 9, 2003.

⁴⁰ Mandrake Linux Security Update Advisory, November 28, 2003.

⁴¹ SuSE Security Announcement, SuSE-SA:2003:048, December 3, 2003.

⁴² Conectiva Linux Security Announcement, CLA-2003:798, December 9, 2003.

⁴³ Red Hat Security Advisory, RHSA-2003:390-0, December 11, 2003.

⁴⁴ Hewlett-Packard Company Security Bulletin, HPSBUX0312-304, December 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM ⁴⁵	Windows 2000, Unix	Directory Server 4.1	A Cross-Site Scripting vulnerability exists via the web administrative interface due to insufficient validation, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Directory Server Web Administration Interface Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, an exploit has been published.
IlohaMail ⁴⁶	Multiple	IlohaMail 0.7.0-0.7.9, 0.8.6-0.8.10	A Cross-Site Scripting vulnerability exists when handling user-supplied parameters due to insufficient verification, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	IlohaMail Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Jason Maloney ⁴⁷	Unix	Guest book 3.0	A vulnerability exists in the 'name' field due to insufficient sanitization, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	Guestbook HTML Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Jason Maloney ⁴⁸	Windows, Unix	Guest-book 3.0	A vulnerability exists due to an input validation error when handling POST requests, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Guestbook Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit has been published..
Kai Banken-horn ⁴⁹	Unix	Bitfolge sniff 1.2.6	A Cross-Site Scripting vulnerability exists due to a failure to verify the 'path' parameter, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Bitfolge Snif Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Kai Blankenhorn ⁵⁰	Windows, Unix	Bitfolge sniff 1.0, 1.1 a, 1.1-1.2.1	A Directory Traversal vulnerability exists due to insufficient sanitization of URI parameters, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.bitfolge.de/download/snif_125.zip?KONTE=NTSID=c3d10680d864a34ac01bc2834db63751	Bitfolge Snif Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Land Down Under ⁵¹	Windows, Unix	Land Down Under 601	A vulnerability exists in the 'auth.php' script due to insufficient validation, which could let a remote malicious user bypass authentication to obtain unauthorized access.	Upgrade available at: http://ldu.neocrome.net/page.php?id=1249	Land Down Under 'Auth.PHP' Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

⁴⁵ Bugtraq, December 2, 2003.

⁴⁶ Secunia Advisory, SA10320, December 1, 2003.

⁴⁷ Bugtraq, December 5, 2003.

⁴⁸ Bugtraq, December 3, 2003.

⁴⁹ Securiteam, December 9, 2003.

⁵⁰ SecurityFocus, November 27, 2003.

⁵¹ SecurityTracker Alert, 1008416, December 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Linksys ⁵²	Multiple	WRT54G v1.0 1.42.3 (Firmware)	A Denial of Service vulnerability exists when handling blank HTTP GET requests.	No workaround or patch available at time of publishing.	WRT54G Router Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Mambo ⁵³	Windows, Unix	Mambo Open Source 4.0.14	A vulnerability exists in the 'mambo/articles.php' script in the 'show()' function due to insufficient validation, which could let a malicious user obtain administrative access	No workaround or patch available at time of publishing.	Mambo Server Input Validation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mambo ⁵⁴	Windows, Unix	Mambo Open Source 4.5 BETA 1.0.3	Multiple vulnerabilities exist: a vulnerability exist in 'pollBooth.php' in the 'dbprefix' parameter due to insufficient verification, which could let a malicious user obtain unauthorized access; and a vulnerability exists in 'articles.php' in the 'artid' parameter due to insufficient verification, which could let a malicious user obtain manipulate the database.	The vendor has issued version 4.5 Beta 1.0.4 to correct the vulnerabilities in 4.5 Beta 1.0.3.	Mambo Server Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mantis ⁵⁵	Unix	Mantis 0.9, 0.9.1, 0.10-0.10.2, 0.11, 0.11.1, 0.12, 0.13, 0.13.1, 0.14-0.14.8, 0.15-0.15.12, 0.16-0.16.1, 0.17-0.17.5, 0.18 a1, 0.18 0rc1, 0.18 0a2-0.18 0a4	Multiple Cross-Site Scripting vulnerabilities exist due to the way some types of input is handled, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: http://sourceforge.net/projects/showfiles.php?group_id=14963	Mantis Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

⁵² SecurityFocus, December 3, 2003.

⁵³ SecurityTracker Alert, 1008441, December 11, 2003.

⁵⁴ Security Corporation Security Advisory, SCSA-023, December 10, 2003.

⁵⁵ Secunia Advisory, SA10380, December 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Martin K. Peterson 56, 57, 58 <i>Conectiva issues another advisory</i> ⁵⁹	Unix	GDM 2.2.5.4, 2.4.1, 2.4.1.1-2.4.1.6, 2.4.4	Multiple vulnerabilities exist: a Denial of Service vulnerability exists when a malicious user submits an arbitrary number of bytes to GDM; and a Denial of Service vulnerability exists due to a failure to impose a timeout when queering for certain commands.	Upgrade available at: http://ftp.gnome.org/pub/GNOME/sources/gdm/2.4/ <u>Conectiva:</u> Ftp://atualizacoes.conectiva.com.br/ <u>Mandrake:</u> Http://www.mandrakesecurity.net/en/ftp.php <u>Slackware:</u> ftp://ftp.slackware.com/pub/slackware/	Multiple GDM Denial of Service CVE Names: CAN-2003-0793, CAN-2003-0794	Low	Bug discussed in newsgroups and websites.
Microsoft ⁶⁰	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Data-center Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, XP Home, SP1, XP Media Center Edition, XP Professional, SP2	A vulnerability exists in Proquota, which could let a malicious user bypass profile storage limits.	No workaround or patch available at time of publishing.	Microsoft Proquota Storage Bypass	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

⁵⁶ Mandrake Linux Security Update Advisory, MDKSA-2003:100, October 16, 2003.

⁵⁷ Conectiva Linux Security Announcement, CLA-2003:766, October 17, 2003.

⁵⁸ Slackware Security Bulletin, SA:2003-300-01, October 27, 2003.

⁵⁹ Conectiva Linux Security Advisory, CLSA-2003:792, November 27, 2003.

⁶⁰ SecurityFocus, December 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶¹	Windows 2003	Exchange Server 2003, Windows Server 2003 Data-center Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, Windows Share Point Services 2.0	A vulnerability exists in Microsoft Exchange 2003 when used with Outlook Web Access and Windows SharePoint Services because the deployment causes Kerberos authentication to be disabled in Internet Information Services (IIS), which could let a remote malicious user obtain full access to a random user's mailbox.	Workaround available at: http://www.microsoft.com/exchange/support/e2k3owa.asp	Exchange Server 2003 Outlook Web Access Incorrect Mail Access	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft ⁶² <i>Microsoft updates bulletin & another exploit published</i> ⁶³ <i>Another exploit script published</i> ⁶⁴	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Data center Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Media Center Edition, XP Professional, SP1	A buffer overflow vulnerability exists in 'WKSSVC.DLL' due to the way requests are handled, which could let a remote malicious user execute arbitrary code. <i>V1.1: Updated the File Manifest and Restart Requirement sections for Windows 2000.</i> <i>V1.2: Updated Information Relating to the Windows XP Security Update.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-049.asp	Windows Workstation Service Remote Buffer Overflow CVE Name: CAN-2003-0812	High	Bug discussed in newsgroups and websites. Exploit scripts have been published. <i>Another exploit script has been published.</i>

⁶¹ SecurityTracker Alert, 1008324, November 28, 2003.

⁶² Microsoft Security Bulletin, MS03-049, November 11, 2003.

⁶³ Microsoft Security Bulletin, MS03-049 V1.1 & 1.2, November 11 & 19 2003.

⁶⁴ SecurityFocus, December 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mike Reed ⁶⁵	Unix	Guest book 1.2	Multiple vulnerabilities exist: a vulnerability exists due to a failure to verify if the user is logged in, which could let an unauthorized malicious user obtain administrative access; a vulnerability exists because the name of the guest book data file is not properly verified, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the administrative password is written in a "hidden" HTML field, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	RNN Guestbook Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser. Exploit script has been published.
Moin Moin ⁶⁶	Multiple	Moin Moin 0.1-0.3, 0.7-0.11, 1.0	Two Cross-Site Scripting vulnerabilities exist, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=8482	MoinMoin Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors ⁶⁷	Windows 95/98/ME/NT 4.0/2000, 2003, XP	Microsoft Internet Explorer 5.0, 5.0.1, SP1-SP3, 5.5, SP1 & SP2, 6.0, SP1, Outlook Express 4.0, 4.0.1 SP2, 4.27.3110, 4.72.2106, 4.72.3120, 4.72.3612, 5.0.1, 5.0, 5.5, 6.0, XP; Mozilla Browser 1.2.1	A vulnerability exists due to the way Internet Explorer displays URLs in the address bar, which could let a remote malicious user spoof the URL address.	No workaround or patch available at time of publishing.	Multiple Browser URI Spoofing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit script has been published. Vulnerability has appeared in the press and other public media.

⁶⁵ Bugtraq, November 27, 2003.

⁶⁶ Secunia Advisory, SA10318, December 1, 2003.

⁶⁷ Bugtraq, December 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁶⁸ <i>More vendors issue advisories</i> ^{69, 70, 71} <i>Turbo Linux issues advisory</i> ⁷²	Unix	GNU glibc 2.3.2, Zebra 0.91a, 0.92a, 0.93b, 0.93a; Quagga Routing Software Suite 0.96.2; RedHat Advanced Workstation for the Itanium Processor 2.1, Enterprise Linux WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1	A Denial of Service vulnerability exists in applications that implement the 'getifaddrs()' function because it is possible to spoof messages sent to the kernel netlink interface.	<u>RedHat:</u> ftp://updates.redhat.com/ <u>SGI:</u> ftp://patches.sgi.com/support/free/security/advisories <u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/9/ <u>OpenPKG:</u> ftp://ftp.openpkg.org/release <u>TurboLinux:</u> ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32	Spoofed Kernel Netlink Interface Message Denial of Service CVE Name: CAN-2003-0859	Low	Bug discussed in newsgroups and websites.
Multiple Vendors ⁷³	Unix	Linux kernel 2.4.0-test1-test12, 2.4-2.4.22	A vulnerability exists in the kernel real time clock interface procedures, which could let a malicious user obtain sensitive information.	<u>SuSE:</u> ftp://ftp.suse.com/pub/suse/	Linux Kernel Memory Disclosure	Medium	Bug discussed in newsgroups and websites.

⁶⁸ Red Hat Security Advisory, RHSA-2003: 325-01, 315-08, 317-08, 305-12, & 307-01, November 12 & 13, 2003.

⁶⁹ SGI Security Advisory, 20031101-01-U, November 19, 2003.

⁷⁰ Conectiva Linux Security Announcement, CLA-2003:786, November 20, 2003.

⁷¹ OpenPKG Security Advisory, OpenPKG-SA-2003.049, November 25, 2003.

⁷² Turbolinux Security Announcement, December 6, 2003.

⁷³ SuSE Security Announcement, SuSE-SA:2003:049, December 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 74, 75</p> <p><i>Exploit script published & more advisories issued</i>^{76, 77, 78, 79}</p> <p><i>More advisories issued</i>^{80, 81}</p> <p><i>Turbo Linux issues advisory</i>⁸²</p>	Unix	<p>GNU fileutils 4.0, 4.0.36, 4.1, 4.1.6, 4.17;</p> <p>Washington University wu-ftp 2.4.1, 2.4.2</p> <p>academ BETA1-15, BETA-18, 2.4.2</p> <p>VR10 -VR17, 2.5.0, 2.6.0-2.6.2</p>	An integer overflow vulnerability exists in /bin/ls, which could let a remote malicious user cause a Denial of Service.	<p>Patches available at: http://mail.gnu.org/archive/html/bug-coreutils/2003-10/msg00070.html</p> <p><u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/</p> <p><u>Immunix:</u> http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/fileutils-4.0x-3_imnx_3.i386.rpm</p> <p><u>Mandrake:</u> http://www.mandrakesecure.net/en/ftp.php</p> <p><u>RedHat:</u> ftp://updates.redhat.com/</p> <p><u>SGI:</u> ftp://patches.sgi.com/support/free/security/advisories</p> <p><u>Trustix:</u> http://http.trustix.org/pub/trustix/updates/</p> <p><u>TurboLinux:</u> ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</p>	<p>Coreutils LS Width Argument Remote Denial of Service</p> <p>CVE Name: CAN-2003-0853</p>	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, an exploit script has been published.

⁷⁴ Georgi Guninski Security Advisory #62, October 22, 2003

⁷⁵ Conectiva Linux Security Announcement, CLA-2003:768 & CLA-2003:771, October 22 & 24, 2003.

⁷⁶ Immunix Secured OS Security Advisory, IMNX-2003-7+-026-01, October 31, 2003.

⁷⁷ Red Hat Security Advisories, RHSA-2003:309-01 & RHSA-2003:310-10, November 3 & 12, 2003.

⁷⁸ SecurityFocus, November 13, 2003.

⁷⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:106, November 13, 2003.

⁸⁰ SGI Security Advisory, 20031101-01-U, November 19, 2003.

⁸¹ Trustix Secure Linux Security Advisory, TLSA-2003-0042, November 17, 2003.

⁸² Turbolinux Security Advisory ,TLA-2003-60, November 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors⁸³</p> <p><i>Exploit script published and more upgrades issued^{84, 85, 86}</i></p> <p><i>More advisories issued^{87, 88, 89}</i></p> <p><i>Conectiva issues another advisory⁹⁰</i></p>	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4-2.4.17, 2.4.18, 2.4.18 x86, 2.4.18 pre-1-2.4.18 pre-8, 2.4.19, 2.4.19 - pre1-2.4.19 - pre6, 2.4.20, 2.4.21, 2.4.21 pre1, 2.4.21 pre4	<p>Multiple vulnerabilities exist: an information disclosure vulnerability exists due to a flaw in 'proc/tty/driver/serial,' which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists due to a race condition in the execve() system call; an access control vulnerability exists because a malicious user can bind services to UDP ports that have already been allocated; an access control vulnerability exists in the 'execve()' because the file descriptor of an executable process is recorded in the calling process's file table, which could let a malicious user obtain sensitive information; a vulnerability exists in the '/proc' filesystem, which could let a malicious user obtain sensitive information; a remote Denial of Service vulnerability exists in the Spanning Tree Protocol (STP) implementation due to insufficient validation of user-supplied input; a vulnerability exists because the bridge topology can be modified due to the inherent insecurity of the STP protocol, which could let a remote malicious user modify information; and a vulnerability exists in the forwarding table, which could let a remote malicious user spoof packets.</p>	<p>Engarde: http://infocenter.guardiandigital.com/advisories/</p> <p>RedHat: ftp://updates.redhat.com/</p> <p>Conectiva: ftp://ul.conectiva.com.br/updates/</p> <p>Debian: http://security.debian.org/pool/updates/main/k/</p> <p>Mandrake: http://www.mandrakesecure.net/en/advisories/</p> <p>SuSE: http://www.suse.de/de/private/download/updates/index.html</p> <p>Debian: http://security.debian.org/pool/updates/main/k/</p> <p>RedHat: ftp://updates.redhat.com/</p>	<p>Multiple Linux 2.4 Kernel Vulnerabilities</p> <p>CVE Names: CAN-2003-0461, CAN-2003-0462, CAN-2003-0464, CAN-2003-0476, CAN-2003-0501, CAN-2003-0550, CAN-2003-0551, CAN-2003-0552</p>	<p>Low/Medium</p> <p>(Medium if sensitive information can be obtained or elevated privileges are obtained)</p>	<p>Bug discussed in newsgroups and websites.</p> <p><i>Proof of Concept exploit has been published for the execve() system call Denial of Service.</i></p>

⁸³ Red Hat Security Advisory, RHSA-2003:238-01, July 21, 2003.

⁸⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:074, July 15, 2003.

⁸⁵ Conectiva Linux Announcement, CLSA-2003:712, July 28, 2003.

⁸⁶ Debian Security Advisories, DSA 358-21 & DSA 358-2, July 31, 2003 & August 5, 2003.

⁸⁷ SuSE Security Announcement, SuSE-SA:2003:034, August 12, 2003.

⁸⁸ Debian Security Advisory, DSA 358-4, August 13, 2003.

⁸⁹ RedHat Security Advisories, RHSA-2003:198-16 & 239-13, August 21, 2003.

⁹⁰ Conectiva Linux Security Announcement, CLA-2003:796, December 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁹¹ <i>Vendors issues updates</i> ^{92, 93} <i>Conectiva issues another advisory</i> ⁹⁴	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4-2.4.17, 2.4.18, 2.4.18 x86, 2.4.18 pre-1-2.4.18 pre-8, 2.4.19, 2.4.19 - pre1-2.4.19 pre6, 2.4.20, 2.4.21, 2.4.21 pre1, 2.4.21 pre4	A remote Denial of Service vulnerability exists in the 'decode_fh' function in 'nfs3xdr.c' due to a failure to handle a negative size value in certain NFS calls.	<u>Debian:</u> http://security.debian.org/pool/updates/main/k <u>Conectiva:</u> http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000730 <u>RedHat:</u> http://www.redhat.com/	Linux Kernel 2.4 'nfsxdr.c' Remote Denial of Service CVE Name: CAN-2003-0619	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

⁹¹ Bugtraq, July 29, 2003.

⁹² Conectiva Security Announcement, CLSA-2003:730, September 1, 2003.

⁹³ RedHat Security Advisories, RHSA-2003:198-17, RHSA-2003:239-13, August 21, 2003.

⁹⁴ Conectiva Linux Security Announcement, CLA-2003:796, December 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{95, 96, 97, 98, 99, 100, 101, 102, 103, 104}	Unix	Astaro Security Linux 4.016, 4.008; Linux kernel 2.4-2.4.22, 2.5.0-2.5.69, 2.6-test1-test6; Trustix Secure Linux 2.0	A vulnerability exists in the 'do_brk()' function due to insufficient sanity checking when handling address data, which could let a malicious user obtain root access.	Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/k/ Linux Kernel: ftp://ftp.kernel.org/pub/linux/kernel/v2.4/linux-2.4.23.tar.gz Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ YellowDog: ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/	Linux Kernel 'do_brk()' Function Root Access CVE Name: CAN-2003-0961	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

⁹⁵ Debian Security Advisory, DSA-403-1, December 1, 2003.

⁹⁶ Mandrake Linux Security Update Advisory, MDKSA-2003:110, December 1, 2003.

⁹⁷ Trustix Secure Linux, TLSA-2003-0046, December 1, 2003

⁹⁸ Slackware Security Advisories, SSA:2003-336-01 & SSA:2003-336-01b, December 2, 2003.

⁹⁹ Red Hat Security Advisories, RHSA-2003:389-07 & RHSA-2003:392-00, December 1 & 2, 2003.

¹⁰⁰ SGI Security Advisory, 20031201-01-A, December 2, 2003.

¹⁰¹ Yellow Dog Linux Security Announcement, YDU-20031203-1, December 3, 2003.

¹⁰² Turbolinux Security Announcement, TLSA-2003-12-03, December 3, 2003.

¹⁰³ SuSE Security Announcement, SuSE-SA:2003:049, December 4, 2003.

¹⁰⁴ Conectiva Linux Security Announcement, CLA-2003:796, December 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117	Unix	EnGarde Secure Community 1.0.1, 2.0, Secure Professional 1.1, 1.2, 1.5; RedHat rsync- 2.4.6- 2.i386. rpm, 2.4.6- 5.i386. rpm, 2.4.6- 5.ia64. rpm, 2.5.4- 2.i386. rpm, 2.5.5- 1.i386 .rpm, 2.5.5- 4.i386. rpm, rsync rsync 2.3.1, 2.3.2, 2.4.0, 2.4.1, 2.4.3- 2.4.6, 2.4.8, 2.5.0- 2.5.6; SGI ProPack 2.3; Slackware Linux – current, Linux 8.1, 9.0, 9.1	A vulnerability exists when running in daemon mode, which could let a remote malicious user execute arbitrary code. <i>NOTE: This vulnerability has already been exploited to compromise servers on the Internet in combination with a Linux privilege escalation vulnerability.</i>	Conectiva: ftp://atualizacoes.conectiva.com.br/8 Debian: http://security.debian.org/pool/updates/main/r/rsync Engarde: http://infocenter.guardiandigital.com/advisories/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Immunix: http://download.immunix.org/ImmunixOS/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/1.3/UPD/rsync-2.5.6-1.3.1.src.rpm RedHat: ftp://updates.redhat.com/ Rsync: http://samba.org/ftp/rsync/rsync-2.5.7.tar.gz SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/ Slackware: ftp://ftp.slackware.com/pub/slackware/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/	RSync Daemon Mode Remote Heap Overflow CVE Name: CAN-2003-0962	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹⁰⁵ Conectiva Linux Security Announcement, CLA-2003:794, December 4, 2003.

¹⁰⁶ Debian Security Advisory, DSA 404-1, December 4, 2003.

¹⁰⁷ Mandrake Linux Security Update Advisory, MDKSA-2003:111, December 4, 2003.

¹⁰⁸ OpenPKG Security Advisory, OpenPKG-SA-2003.051, December 4, 2003.

¹⁰⁹ Guardian Digital Security Advisory, ESA-20031204-032, December 4, 2003.

¹¹⁰ Trustix Secure Linux Security Advisory, 2003-0048, December 4, 2003.

¹¹¹ Red Hat Security Advisories, RHSA-2003:398-0 & RHSA-2003:399-06, December 4, 2003.

¹¹² Slackware Security Advisory, SSA:2003-337-01, December 4, 2003.

¹¹³ SuSE Security Announcement, SuSE-SA:2003:050, December 4, 2003.

¹¹⁴ Fedora Security Update Notification, FEDORA-2003-030, December 4, 2003.

¹¹⁵ Immunix Secured OS Security Advisory, IMNX-2003-73-001-01, December 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
myServer ¹¹⁸	Windows	myServer 0.2, 0.4.1-0.4.3, 0.5, 0.11	A remote Denial of Service vulnerability exists due to a boundary error when handling requested resource names.	Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=63119	MyServer Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
NeoStats Software Group ¹¹⁹	Unix	NeoStats 2.5-2.5.9	A vulnerability exists due to an incompatibility with legacy umodes that are supported by NeoStats and new umodes that have been introduced in the latest version of UnrealIRCd, which could let a remote malicious user obtain elevated privileges.	Upgrade available at: http://www.dynam.ac/members/sitescripts/counter/dlcount.php?id=neostats&url=http://www.neostats.net/NeoStats-2.5.10.tar.gz	NeoStats For Unreal IRCd Elevated Privileges	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NetGear ¹²⁰	Multiple	NetGear WAB102 Wireless Access Point Firmware 1.2.3	An authentication vulnerability exists, which could let a remote malicious user obtain unauthorized access. In addition, a power failure resets the device to a known password, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	NetGear WAB102 Wireless Access Point Password Management	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NetScreen Technologies, Inc. ¹²¹	Multiple	ScreenOS 4.0, r1-r12, 4.0.1, r1-r10, 4.0.2, 4.0.3, 4.1-r4	A vulnerability exists because timed out sessions are not properly handled, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://www.netscreen.com/sitemap.jsp	ScreenOS Session Timeout Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Net-X Solutions ¹²² <i>Upgrade now available</i> ¹²³	Windows	NetServe Web Server 1.0.7	Several vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient sanitization, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because the software stores the administrator's username and password in the 'config.dat' file, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.starlots.com/netx/index.html	NetServe Web Server Directory Traversal & Password Storage	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹¹⁶ Turbolinux Security Announcement, December 6, 2003.

¹¹⁷ SGI Security Advisory, 20031202-01-U, December 10, 2003.

¹¹⁸ SecurityFocus, December 8, 2003.

¹¹⁹ SecurityTracker Alert, 1008454, December 12, 2003.

¹²⁰ Bugtraq, December 10, 2003.

¹²¹ Bugtraq, December 5, 2003.

¹²² Bugtraq, November 17, 2003.

¹²³ SecurityFocus, December 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell ¹²⁴	Multiple	Netware 6.5, 6.5 SP1	A vulnerability exists because NFS Server (XNFS.NLM) does not handle hostname aliases correctly in trusted host's configuration, which could let a remote malicious user bypass access controls.	Patch available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10089375.htm	Novell NFS Server Hostname Alias CVE Name: CAN-2003-0976	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenCA ¹²⁵	Unix	OpenCA 0.8.0, 0.8.1, 0.8.6, 0.9.0-0.9.0-2, 0.9.1-0.9.1 -3	Multiple vulnerabilities exist: a vulnerability exists due to errors in the regular expressions in 'OpenCA::PKCS7,' and in the 'crypto-utils.lib' library when creating X.509 objects and when checking serials of certificates used for creating a PKCS#7 signature, which could let a local/remote malicious user that has an invalid or revoked certificate obtain unauthorized access.	Upgrades available at: http://www.openca.org/cgi-bin/openca/downloads/sf-dl?name=openca-0.9.1-4.tar.gz	OpenCA Signature Verification Vulnerabilities CVE Name: CAN-2003-0960	Medium	Bug discussed in newsgroups and websites.
Paul L Daniels ¹²⁶	Unix	Ebola 0.1.4	A buffer overflow vulnerability exists in the 'handle_PASS()' function during user authentication, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://pldaniels.com/ebola/ebola-0.1.5.tar.gz	Ebola Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
phpBB Group ¹²⁷	Windows, Unix	PhpBB 2.0.6	A vulnerability exists in the 'search_id' parameter due to insufficient verification, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.phpbb.com/	phpBB 'search.php' Input Validation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

¹²⁴ Novell Technical Information Document, TID10089375, December 4, 2003.

¹²⁵ OpenCA Security Advisory, November 28, 2003.

¹²⁶ Secure Network Operations, Inc. Advisory, SRT2003-12-04-0723, December 4, 2003.

¹²⁷ Secunia Advisory, SA10308, November 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Postgre SQL ¹²⁸ <i>Vendors issue advisories</i> ^{129, 130} <i>More advisories issued</i> ^{131, 132, 133, 134, 135} <i>More advisories issued</i> ^{136, 137} <i>Turbo Linux issues advisory</i> ¹³⁸	Unix	Postgre SQL 7.2-7.2.4, 7.3-7.3.3	A buffer overflow vulnerability exists in the 'PostgreSQL to_ascii()' function, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.postgresql.org/Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000772 OpenPKG: ftp://ftp.openpkg.org/release/1.2/UPD/ Debian: http://security.debian.org/pool/updates/main/p/postgresql/ Mandrake: http://www.mandrakesecurity.net/en/advisories/ OpenPKG: ftp://ftp.openpkg.org/release/1.2/UPD/ RedHat: ftp://updates.redhat.com/ SGI: ftp://patches.sgi.com/support/free/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/	PostgreSQL To_Ascii() Buffer Overflow CVE Name: CAN-2003-0901	High	Bug discussed in newsgroups and websites.

¹²⁸ SecurityFocus, October 1, 2003.

¹²⁹ Conectiva Linux Announcement, CLSA-2003:772, October 24, 2003.

¹³⁰ OpenPKG Security Advisory, OpenPKG-SA-2003.047, October 30, 2003.

¹³¹ Mandrake Linux Security Update Advisory, MDKSA-2003:102, November 4, 2003.

¹³² Debian Security Advisory, DSA 397-1, November 7, 2003.

¹³³ OpenPKG Security Advisory, OpenPKG-SA-2003.048, November 11, 2003.

¹³⁴ Conectiva Linux Security Announcement, CLA-2003:784, November 13, 2003.

¹³⁵ Red Hat Security Advisories, RHSA-2003:314-08 & 313-00, November 12 & 13, 2003.

¹³⁶ Trustix Secure Linux Security Advisory, TSLSA-2003-0040, November 17, 2003.

¹³⁷ SGI Security Advisory, 20031101-01-U, November 19, 2003.

¹³⁸ Turbolinux Security Advisory, TLSA-2003-62, November 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat ¹³⁹ <i>Conectiva issues advisory</i> ¹⁴⁰ <i>More vendors issue advisories</i> ^{141, 142, 143} <i>Turbo Linux issues advisory</i> ¹⁴⁴	Unix	Enterprise Linux WS 2.1 IA64, 2.1, ES 2.1 IA64, 2.1, AS 2.1 IA64, 2.1	A buffer overflow vulnerability exists in the 'getgrouplist' function if the size of the group list is too small to hold all the user's groups, which could let a malicious user cause a Denial of Service.	Patches available at: http://rhn.redhat.com/errata/RHSA-2003-249.html <i>Conectiva:</i> ftp://atualizacoes.conectiva.com.br/ <i>Mandrake:</i> http://www.mandrakesecurity.net/en/advisories/ <i>RedHat:</i> ftp://updates.redhat.com/ <i>Trustix:</i> http://www.trustix.org/errata/misc/2003/TSL-2003-0039-glibc.asc.txt <i>TurboLinux:</i> ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/	Glibc Getgrouplist Function Buffer Overflow CVE Name: CAN-2003-0689	Low	Bug discussed in newsgroups and websites.
RedHat ¹⁴⁵	Unix	Linux kernel 2.4-2.4.22	A Denial of Service vulnerability exists when an error is returned on a concurrent fork().	Fedora http://download.fedora.redhat.com/pub/fedora/linux/core/updates/	Linux Kernel Denial of Service	Low	Bug discussed in newsgroups and websites.
Sebastian Hoffmann ¹⁴⁶	Unix	BNCWeb	A file disclosure vulnerability exists in the 'BNCquery.pl' script, which could let a remote malicious user obtain sensitive information.	Workaround: The author has recommended removing lines removing lines 23 to 25 in the BNCquery.pl script.	BNCWeb 'BNCquery.pl' File Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹³⁹ RedHat Security Advisory, RHSA-2003:249-11, August 22, 2003.

¹⁴⁰ Conectiva Linux Security Announcement, CLA-2003:762, October 14, 2003.

¹⁴¹ Red Hat Security Advisory, RHSA-2003:325-01, November 13, 2003.

¹⁴² Mandrake Linux Security Update Advisory, MDKSA-2003:107, November 19, 2003.

¹⁴³ Trustix Secure Linux Security Advisory, TSLSA-2003-0039, November 17, 2003.

¹⁴⁴ Turbolinux Security Announcement, December 5, 2003.

¹⁴⁵ Fedora Security Update Notification, FEDORA-2003-026, December 2, 2003.

¹⁴⁶ Bugtraq, December 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI ¹⁴⁷ <i>SGI updates advisory¹⁴⁸</i>	Unix	IRIX 6.5-6.5.22, 6.5.17 m- 6.5.21 m, 6.5.17 f- 6.5.21 f	Multiple vulnerabilities exist: a vulnerability exists because a remote malicious user may be able to mount a file system via an unprivileged port even if rpc.mountd is started with the '-n' option; a remote Denial of Service vulnerability exists in 'rpc.mountd' which would make NFS services unavailable; and a vulnerability exists because the 'rpc.mountd' service returns various replies depending on whether a requested file exists or not, which could let a malicious user obtain sensitive information. <i>The original patches 5387-5389 had a format mismatch between exportfs and rpc.mountd. New patches 5426-5429 have been released to fix this mismatch. (SGI BUG 902638)</i>	Patches available at: ftp://patches.sgi.com/support/free/security/patches	SGI rpc.mountd Multiple Vulnerabilities CVE Name: CAN-2003-0796, CAN-2003-0797	Low/Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
STAL-LION Networking ¹⁴⁹	Multiple	Cyclonic webmail 4.0	A vulnerability exists due to a flaw in the procedure used to authenticate a remote user before Cyclonic webmail scripts are available for perusal/use, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Cyclonic Webmail Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Stunnel ¹⁵⁰ <i>More advisories issued^{151, 152, 153}</i>	Windows 98/ 2000, Unix	Stunnel 3.20. 3.10. 3.3, 3.4 a, 3.7-3.9, 3.11-3.19, 3.21, a, b, c, 3.22, 3.24, 4.0	A vulnerability exists in the 'listen()' call because returned file descriptors are made available to unprivileged processes, which could let a malicious user hijack the Stunnel Server.	STunnel: http://www.stunnel.org/download/stunnel/src/stunnel-4.04.tar.gz Mandrake: http://www.mandrakesecurity.net/en/mlist.php RedHat: ftp://updates.redhat.com/ SGI: http://www.sgi.com/support/security/	Stunnel Leaked File Descriptor CVE Name: CAN-2003-0740	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁴⁷ SGI Security Advisory, 20031102-01-P, November 21, 2003.

¹⁴⁸ SGI Security Advisory, 20031102-02-P, December 5, 2003.

¹⁴⁹ SecurityFocus, December 10, 2003.

¹⁵⁰ Conectiva Linux Security Announcement, CLA-2003:736, September 5, 2003.

¹⁵¹ Red Hat Security Advisory, RHSA-2003:296-01, November 24, 2003.

¹⁵² Mandrake Linux Security Update Advisory, MDKSA-2003:108, November 25, 2003.

¹⁵³ SGI Security Advisory, 20031103-01-U, November 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc. ¹⁵⁴	Unix	Cluster 2.2, 3.0, 3.1	A Denial of Service vulnerability exists when a client application is running that uses a TCP port.	Workaround available at: http://sunsolve.sun.com/pub/cgi/retrieve.pl?doc=fsalert%2F57428	Sun Cluster TCP Port Conflict Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc. ¹⁵⁵	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists in the Xsun(1) Solaris X11 server when run in Direct Graphics Access (DGA) mode, which could let a malicious user cause a Denial of Service or obtain elevated privileges.	Patches available at: http://sunsolve.sun.com	Sun Solaris XSun Direct Graphics Access	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc. ¹⁵⁶	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A buffer overflow vulnerability exists in 'dtprintinfo' due to the way strings are handled, which could let a malicious user execute arbitrary code.	Patches available at: http://sunsolve.sun.com	CDE DTPrintInfo Buffer Overflow	High	Bug discussed in newsgroups and websites.
Sun ONE/iPlanet ¹⁵⁷	Windows NT 4.0/2000, Unix	iPlanet Web Server 4.1, SP1-SP12, 6.0, SP1-SP5; Sun ONE Web Server 4.1, SP10-SP12, 6.0, SP1-SP5;	A remote Denial of Service vulnerability exists in the Sun ONE/iPlanet web server.	<u>IPlanet:</u> http://www.sun.com/software/download/products/3f8472da.html <u>Sun One:</u> http://www.sun.com/software/download/products/3f8472da.html	Sun ONE/iPlanet Web Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Surfboard ¹⁵⁸	Unix	Surfboard httpd 1.1.8	Two vulnerabilities exist: a Directory Traversal vulnerability exists due to insufficient input validation, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a malicious user connects to the service and then closes it again without sending any data.	No workaround or patch available at time of publishing.	Surfboard Web Server Directory Traversal & Denial of Service	Low/ Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.

¹⁵⁴ Sun(sm) Alert Notification, 57428, November 25, 2003.

¹⁵⁵ Sun(sm) Alert Notification, 57419, December 2, 2003.

¹⁵⁶ Sun(sm) Alert Notification, 57441, December 5, 2003.

¹⁵⁷ Sun(sm) Alert Notification, 57423, December 2, 2003.

¹⁵⁸ Secunia Advisory, SA10327, December 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SuSE ¹⁵⁹	Unix	Linux 9.0	Multiple vulnerabilities exist in xscreensaver packages shipped with SuSE Linux 9.0. These issues include a crash when xscreensaver is handling the verification of authentication credentials and several insecure temporary file creation vulnerabilities.	No workaround or patch available at time of publishing.	SuSE XScreenSaver Package Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
SuSE ¹⁶⁰ <i>Exploit script published.</i> ¹⁶¹	Unix	Linux Professional 8.2	A vulnerability exists in the SuSEWM configuration file used by SuSEConfig, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	SuSE Linux SuSEWM Configuration File	Medium	Bug discussed in newsgroups and websites.
Sybase ¹⁶²	Windows NT 4.0/2000, 2003, XP	Adaptive Server Anywhere 9.0	Multiple vulnerabilities exist: a format string vulnerability exists in the 'XP_SPRINTF' extended stored procedure, which could let a remote malicious user obtain DBA privileges or execute arbitrary code; a vulnerability exists due to boundary errors in multiple 'CREATE,' 'ALTER,' and 'BACKUP' statements, which could let a remote malicious user execute arbitrary code; a vulnerability exists in a couple of other statements, procedures, and stored procedures, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because multiple 'FUNCTIONS' can be exploited to cause a Denial of Service.	Further information can be obtained by contacting the vendor or by logging into the following page. http://downloads.sybase.com/swd/swx/sdsummary.stm?baseprodName=SQL+Anywhere+Studio&baseprod=144&client=swx&previewObj=4&timeframeObj=6	Adaptive Server Anywhere Multiple Remote Buffer Overflow Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Virtual Programming ¹⁶³	Windows 95/98/NT 4.0/2000, XP	VP-ASP 4.0, 5.0	A vulnerability exists in the 'shopsearch.asp' and 'shopdisplayproducts.asp' scripts due to insufficient validation, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	Patches available at: http://www.vpasp.com/virtpro/faq/faq_securityfixes.htm	VP-ASP 'shopsearch' & 'shopdisplayproducts' Scripts SQL Injection	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

¹⁵⁹ SuSE Security Announcement, SuSE-SA:2003:047, November 28, 2003.

¹⁶⁰ Bugtraq, October 6, 2003.

¹⁶¹ SecurityFocus, November 26, 2003.

¹⁶² NGSSoftware Insight Security Research Advisory, December 10, 2003.

¹⁶³ Securiteam, December 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WEB-GATE, Inc. ¹⁶⁴	Multiple	WebEye SPD, E20, E104, E10, B106, B101	An information disclosure vulnerability exists in the '/admin/wg_user-info.ml' script due to insufficient verification of user credentials, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebEye Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Websense ¹⁶⁵	Windows NT 4.0/2000, 2003, Unix	Websense Enterprise 4.3, 4.4, 5.0 1, 5.1	A Cross-Site Scripting vulnerability exists because malicious characters included in an URL are not properly verified when an error is returned in case the site or URL is blocked, which could let a remote malicious user execute arbitrary code.	Patches available at: ftp://ws4:safesurf@ftp2.websense.com/	Websense Enterprise Blocked Sites Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Xoops ¹⁶⁶	Windows, Unix	Xoops 1.3.5-1.3.10, 2.0-2.0.3, 2.0.5	Multiple vulnerabilities exist: an input validation vulnerability exists in 'banners.php' in the '\$cid' variable, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'change_banner_url_by_client()' which could let a remote malicious user modify the URL of banners; and a vulnerability exists in 'edituser.php' and 'imagemanager.php' which could let a remote malicious user redefine various internal variables.	Upgrade available at: http://www.xoops.org/generator/download.php#xoops2	Xoops Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
Yahoo! ¹⁶⁷	Multiple	Messenger 5.5.1249, 5.5, 5.6.1355, 5.6.0.1347, 5.6	A Cross-Site Scripting vulnerability exists in 'ypager.exe' when an invalid IMVironment environment is specified, which could let a remote malicious user execute arbitrary HTML and script code.	Update available at: http://messenger.yahoo.com	Yahoo! Messenger 'ypager.exe' Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Yahoo! ¹⁶⁸	Windows	Messenger 5.6.0.1347, 5.6	A buffer overflow vulnerability exists in 'YAUTO.DLL' ActiveX component, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://messenger.yahoo.com/security/update4.html	Yahoo! Messenger Buffer Overflow	High	Bug discussed in newsgroups and websites.

¹⁶⁴ Securiteam, December 8, 2003.

¹⁶⁵ Bugtraq, December 3, 2003.

¹⁶⁶ Security Corporation Security Advisory, SCSSA-022, December 5, 2003.

¹⁶⁷ Bugtraq, December 5, 2003.

¹⁶⁸ Bugtraq, December 3, 2003.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 28 and December 9, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listserve, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 24 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
December 9, 2003	hole-e-day.zip	Exploit for the Multiple Browser URI Spoofing vulnerability.
December 8, 2003	webeye.pl	Perl script that exploits the WebEye Information Disclosure vulnerability.
December 7, 2003	eZstack.pl	Perl script that exploits the EZMeeting 'EZNet.EXE' Remote Buffer Overflow vulnerability.
December 5, 2003	qwks.cpp	Script that exploits the Windows Workstation Service Remote Buffer Overflow vulnerability.
December 5, 2003	I2S-LAB-10-15-03.Shell32-Do.txt	Exploit and research for the Microsoft Windows 2000 SHELL32.DLL Denial of Service.
December 4, 2003	rpc_wks_bo.c	Script that exploits the Windows Workstation Service Remote Buffer Overflow vulnerability.
December 4, 2003	eZpsheap.pl	Perl script that exploits the Multiple EZPhotoShare Memory Corruption Vulnerabilities.
December 4, 2003	0x333ebola.c	Script that exploits the Ebola Buffer Overflow vulnerability.
December 3, 2003	JMaloneyGB-exp.	Exploit for the Guestbook Remote Command Execution vulnerability.
December 2, 2003	brk_poc.asm	Proof of Concept exploit for the Linux Kernel 'do_brk()' Function Root Access vulnerability.
December 2, 2003	brian.c	A simple tool to effectively convert a switched network (or a part of it) into a shared network so that sniffing can take place.
December 2, 2003	f.c	Script that exploits the SuSE Linux SuSEWM Configuration File vulnerability.
December 2, 2003	hydra-2.5.tar.gz	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more.
December 2, 2003	surfboard-1.1.8.txt	Exploit URL for the Surfboard Web Server Directory Traversal vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
December 1, 2003	cain25b44.exe	A password recovery tool for Microsoft Operating Systems that allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.
December 1, 2003	brk_poc.asm	Exploit for the Linux Kernel 'do_brk()' Function Root Access vulnerability.
December 1, 2003	brk_poc2.asm	Exploit for the Linux Kernel 'do_brk()' Function Root Access vulnerability.
November 30, 2003	rnnquest12.txt	Exploits for the RNN Guestbook Multiple Vulnerabilities
November 30, 2003	phpBB206.txt	Exploit for the phpBB 'viewtopic.php' Input Validation vulnerability.
November 30, 2003	hedgehog_poc.zip	Proof of Concept portscanner written in VBA for Excel.
November 30, 2003	appliedsnatch.c	Script that exploits the Applied Watch Command Center Authentication Bypass vulnerability.
November 30, 2003	addrule.c,	Script that exploits the Applied Watch Command Center Detection Rule Modification vulnerability.
November 28, 2003	applied_exp1.c	Script that exploits the Applied Watch Command Center Authentication Bypass & Detection Rule Modification vulnerability.
November 28, 2003	applied_exp2.c	Script that exploits the Applied Watch Command Center Authentication Bypass & Detection Rule Modification vulnerability.

Trends

- The CERT/CC has received reports of several new variants of the 'Mimail' worm.
- The CERT/CC received a number of reports indicating that malicious user are actively exploiting the Microsoft Internet Explorer vulnerabilities described in the "Bugs, Holes & Patches" Table, CyberNotes-2003-24.
- The SANS Twenty Most Critical Internet Security Vulnerabilities list has been published. This updated SANS Top Twenty is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux. For more information see the list located at: <http://www.sans.org/top20/>.
- The National Cyber Security Division (NCS) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting the Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS) vulnerability. For more information, see "Bugs, Holes & Patches" Table and advisory located at: <http://www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm>. The Microsoft advisory is located at: http://www.microsoft.com/security/security_bulletins/ms03-039.asp. Tools have been developed to exploit this vulnerability and there is an increased likelihood that new viruses will emerge soon.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection.

It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available.** The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32.Mimail	Worm	Increase	July 2003
2	W32/Swen	Worm	Increase	September 2003
3	W32/Klez	Worm	Slight Decrease	January 2002
4	Worm_Msblast.A	Worm	Decrease	August 2003
5	W32/Dumaru-A	Worm	Stable	August 2003
6	W32/Sobig	Worm	Return to Table	May 2003
7	W32/Sober.A	Worm	New to Table	November 2003
8	W32/Bugbear	File	Decrease	September 2002
9	W32/Lovegate	Virus	Decrease	February 2003
10	W32/SQLSlammer	Worm	Decrease	January 2003

Note: Note: Virus reporting may be weeks behind the first discovery of infection. A total 623 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 249 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Bursted (Aliases: ACADLISP/Bursted.A, AutoLispScript/Bursted.A) (Virus): This is a virus written for AutoCAD's embedded scripting language, AutoLISP. It replicates in a separate file, "acad.lsp" that is automatically executed by AutoCAD. It does not affect the actual drawing files.

PE_BODIRU.A (Alias: W32.HLLW.BODIRU) (File Infector Virus): This worm propagates through the following popular peer-to-peer, file-sharing applications:

- KaZaA
- KaZaA Lite K++
- eDonkey2000
- eMule

It also performs Denial of Service (DoS) attacks against the following Web sites:

- mess.be
- symantec.com

The worm can corrupt certain files and terminates antiviral related utilities and processes. It may also drop a batch file that utilizes NET.EXE, a common Windows NT-based utility, to share all drives (A to Z) of the infected machine. It runs on Windows 95, 98, ME, NT, 2000 and XP.

PE_MEMAS.A (Aliases: W32.Memas@mm, W32/Memas@MM) (File Infector Worm): This memory-resident, mass-mailing virus arrives as an attachment on e-mail with the following details:

- Subject: Hi Friend
- Message body: Please See The Attachment
- Attachment: <Variable file name>

It gets target recipients from the Microsoft Outlook address book. PE_MEMAS.A infects all .EXE files found in C:\, the Windows folder, and the Windows system folder. It also infects files with the following file names:

- IEXPLORER.EXE
- CCAPP.EXE
- CCREGVFY.EXE

The worm overwrites all other .EXE files with garbage data and displays a message box on Fridays, October, and the fifth day of each month: It runs on Windows 95, 98, ME, NT, 2000, and XP.

PHP.Feast (PHP Virus): This is a polymorphic PHP file-infecting virus. PHP is a server-side scripting language that is used for dynamic Web page generation. This virus will only execute on systems that are running a Web server that have installed and active PHP modules.

W32/Agobot-AW (Aliases: Backdoor.Agobot.3.gen, W32/Gaobot.worm.gen,

W32.HLLW.Gaobot.gen) (Win32 Worm): This is a network worm that also allows unauthorized remote access to the computer via IRC channels. W32/Agobot-AW copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to protect/patch the computer against such attacks please see Microsoft security bulletins MS03-026 and MS03-001. W32/Agobot-AW drops a copy of itself to the Windows system32 folder as winctrl.exe and adds the following registry entries to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Config Loader
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Config Loader

It collects system information and registration keys of popular games that are installed on the computer and attempts to terminate various processes related to anti-virus and security software (e.g. SWEEP95.EXE, BLACKICE.EXE and ZONEALARM.EXE).

W32/Agobot.AY (Aliases: WORM_AGOBOT.AY, W32.HLLW.Gaobot.gen,

Win32.HLLW.Agobot.3) (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. Like its previous AGOBOT variants, this malware also takes advantage of the following vulnerabilities on a target system:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- RPC Locator vulnerability
- IIS5/WEBDAV Buffer Overrun exploit

It also performs the following malicious tasks:

- Attempt to log on to the target machine using any combination of specified user names and passwords
- Steal Windows Product ID and CD keys of many popular games
- Terminate antiviral and security programs, and system files
- Open a random port
- Connect to an Internet Relay Chat (IRC) client server and wait for several malicious commands from a remote user
- Perform flood attacks against target site

This UPX-packed worm runs on Windows 2000 and XP.

Win32/Agobot.AZ (Alias: WORM_AGOBOT.AZ) (Internet Worm): This worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It also uses a long list of passwords to access and propagate into remote machines with weak passwords. This worm functions as a backdoor program. It allows malicious users to access infected machines via IRC

(Internet Relay Chat). It serves as a bot, waiting for commands from remote users. It also terminates certain Windows processes. It runs on Windows 2000 and XP.

Win32/Agobot.BA (Aliases: WORM_AGOBOT.BA, Aliases: Worm.Win32.Agobot.58368.E, Win32.HLLW.Agobot, Backdoor.Agobot.3.gen, W32.HLLW.Gaobot.gen) (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. Like earlier AGOBOT variants, it also exploits the following Windows vulnerabilities to propagate across the network:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates certain processes and steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows 2000 and XP.

Win32/Agobot.BB (Alias: WORM_AGOBOT.BB) (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. It exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antiviral related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It runs only on Windows 2000 and XP.

W32/Agobot-BD (Alias: WORM_AGOBOT.BD) (Win32 Worm): This worm has been reported in the wild. It is an IRC backdoor Trojan and network worm. W32/Agobot-BD is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-BD moves itself to the Windows system folder as Filename.exe and creates the following registry entries so that it is run automatically on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Win Init=<SYSTEM>\Filename.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Win Init=<SYSTEM>\Filename.exe

On NT based versions of Windows, the worm creates a new service named "Win Init" with the startup property set to automatic, so that the service starts automatically each time Windows is started. Each time W32/Agobot-BD is run, it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-BD then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. W32/Agobot-BD attempts to terminate and disable various security related programs and attempts to prevent its own process from being deleted.

W32/Agobot-BG (Alias: WORM_AGOBOT.BG) (Win32 Worm): This worm propagates into machines on the same network by using exploits to the following vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) (Microsoft Security Bulletin MS03-026)
- RPC Locator (Microsoft Security Bulletin MS03-001)
- IIS5/WEBDAV Buffer Overrun (Microsoft Security Bulletin MS03-007)

These vulnerabilities affect systems running Windows NT, 2000, and XP. Refer to the corresponding links for patch information. It also propagates into machines with accessible shares. The worm uses a dictionary of passwords to log on and propagate into inaccessible network machines. It receives commands via IRC. It allows remote users a variety of actions on affected machines including the ability to flood and attack specified sites. It stops specific programs, including security and antiviral applications. It even has a short list of malware programs to terminate. This worm runs on Windows 2000 and XP.

W32/Agobot-BL (Aliases: WORM_AGOBOT.BL, W32.HLLW.Gaobot.BF, Backdoor.Agobot.3.an, W32/Gaobot.AA.worm) (Win32 Worm): This malware has both worm and backdoor capabilities. It exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antiviral related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It runs only on Windows NT, 2000 and XP.

W32/Agobot-EU (Alias: WORM_AGOBOT.EU) (Win32 Worm): This worm exploits certain vulnerabilities to propagate across networks. It takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator Vulnerability

It attempts to log into systems using a list of user names and passwords. This worm then drops a copy of itself in accessed machines. It also terminates antiviral related processes and dropped files by other malware. This worm steals CD keys of certain game applications, then sends gathered data to a remote user via mIRC, a chat application. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows 2000 and XP.

W32/Gogo.cmp (Win32 Worm): This is a companion virus. When an infected file is executed, it renames all *.EXE files to *.EX1. For example, the file "Calc.exe" becomes "Calc .ex1" and now the file "Calc.exe" is a copy of the virus. The virus will search for EXE files on the following drives:

- C:, D:, E:, F:, G:, H:, I:, J:, L:, M:

Files in the %Windir%, and %Sysdir% folder are not infected. In addition, the file IEXPLORE.EXE, is not infected.

W32.HLLW.Bodiru (Win32 Worm): This is a worm that spreads using file-sharing networks. It attempts to perform a Denial of Service (DoS) attack against two particular Internet hosts. The worm is written in Visual Basic and is compressed with ASPack.

W32.HLLW.Epon@mm (Aliases: I-Worm.Epon, W32/Epon@MM) (Win32 Worm): This is a worm that attempts to spread through file-sharing networks and mIRC. It also uses Microsoft Outlook to send itself to all the contacts in the Outlook address book. The e-mail has the following characteristics:

- Subject: Britney Spears poses nude in the Playboy!
- Attachment: Britney Spears.jpg<many spaces>.exe

The worm is written in Microsoft Visual C++ and is packed with UPX.

W32.HLLW.Gaobot.DK (Win32 Worm): This is a worm that uses several exploits to spread. It acts as a spam proxy, using the infected computer to send large numbers of unsolicited e-mails using its own SMTP engine. This worm also opens a backdoor to a predetermined IRC channel. This worm propagates using multiple vulnerabilities, including:

- Weak passwords on network shares
- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026), using TCP ports 135 and 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007), using TCP port 80

W32.HLLW.Gaobot.DK gives a malicious user complete access to your computer. By default, the worm listens on TCP port 63809 and notifies the malicious user through IRC. The worm attempts to terminate various security products and system-monitoring tools.

W32.HLLW.Slideshow (Win32 Worm): This is a worm that spreads through peer-to-peer file sharing programs, and AOL instant messenger. It is written in Visual Basic. When W32.HLLW.Slideshow is executed, it displays the fake error message:

- Err no entry Cptx32.dll. Patch Failed.

And creates the following files:

- C:\Payload.exe: This is detected as W32.HLLW.Slideshow.
- C:\Data: This is a log file for the worm.
- C:\Debug: A temporary file that the worm uses.
- C:\Slideshow.exe: A copy of the main worm executable.
- C:\Windows\MSCVT.exe: A copy of the main worm executable.

The worm adds the value, "MSCVT"="C:\Windows\MSCVT.exe," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the worm runs when you start Windows. If KaZaA is installed on the system, the worm will attempt to place a copy of itself in KaZaA's My Shared Folder. The worm checks for the existence of AOL Instant Messenger Profiles. If it finds them, when you connect to the Internet, the worm searches your Buddy Lists. Then, the worm sends messages to everyone on the list. The messages contain a link to a copy of the worm that is on a specific Web site.

W32.HLLW.Southghost (Win32 Worm): This is a worm that spreads through e-mail and file-sharing networks. The e-mail has the following characteristics:

- Subject: Espero que te llege a tiempo...
- Attachment: BuenasNuevas.doc.pif

The worm is written in Microsoft Visual Basic and packed with Petite.

W32.HLLW.Studd (Alias: W32/Duster) (Win32 Worm): This is a worm that attempts to spread through the KaZaA, IRC, network shares, as well as the mapped network drives. A malicious user can remotely control the infected hosts through IRC. The worm is written in the Delphi programming language.

W32.Kwbot.S.Worm@mm (Alias: Backdoor.IRCBot.gen) (Win32 Worm): This is a mass-mailing variant of W32.Kwbot.Worm. The worm attempts to spread through the KaZaA file-sharing network and uses its own SMTP engine to e-mail itself to contacts in the Windows address book. The e-mail message has the following characteristics:

- Subject: (randomly chosen from a list)
- Attachment: app.exe

W32.Kwbot.S.Worm@mm is packed with UPX v1.20.

W32.Mertian@mm (Win32 Worm): This is a mass-mailing worm that sends itself to contacts in the Microsoft Outlook address book. The e-mail has the following characteristics:

- Subject: want to see my new pic!!!
- Attachment: My_New_pic.doc.exe

It is written in Microsoft Visual Basic, version 6.0.

W32.Midlak@mm (Win32 Worm): This is a mass-mailing worm that spreads through e-mail, IRC, and the KaZaA file-sharing network. It deletes system files and steals information about the computer on which it runs. It is packed with UPX.

W32/Mimail-L (Alias: WORM_MIMAIL.L) (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via e-mail using addresses harvested from the hard drive of the infected computer. All e-mail addresses found on the computer are saved in a file named xu298da.tmp in the Windows folder. In order to run itself automatically when Windows starts up, the worm copies itself to the file svchost.exe in the Windows folder and adds the following registry entry to point to it:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\France

Hidden inside the virus is the following text that does not get displayed:

- *** Made in France. *** virmakers

Explicit language used in e-mails sent by the worm may offend some customers. The e-mails sent by the worm have various characteristics. W32/Mimail-L also attempts Denial of Service attacks targeting:

- www.spamhaus.org
- www.spews.org
- www.register.com
- www.cardcops.com
- www.carderplanet.net
- www.spamcop.net
- www.authorizenet.com
- disney.go.com

W32/Mimail-M (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via e-mail using addresses harvested from the hard drive of the infected computer. All e-mail addresses found on the computer are saved in a file named xjwu2.tmp in the Windows folder. The worm copies itself to the Windows folder with the filename netmon.exe and creates the following registry entry so that this file is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NetMon

W32/Mimail-M can arrive in two different e-mail formats. Some users may find the explicit language used by the worm offensive. . The e-mails sent by the worm have various characteristics. W32/Mimail-M creates a copy of itself named nji2.tmp and a copy of only_for_greg.zip named msi2.tmp, both in the Windows folder. W32/Mimail-M also attempts a denial of service attack targeting:

- darkprofits.com
- darkprofits.net
- darkprofits.cc
- darkprofits.ws
- www.darkprofits.com
- www.darkprofits.net
- www.darkprofits.cc
- www.darkprofits.ws

W32/Scold-A (Aliases: W32/Scold@mm, WORM_SCOLD.A) Iwin32 Worm): This is a mass mailer that uses Microsoft Outlook to spread. It may arrive in the e-mail that contains various subject lines and message text. The attached file will have a filename constructed from the same characters that were used in the subject line, followed by a random number and an SCR extension. When executed W32/Scold-A displays a photo of a seal, copies itself to the Windows folder as Warm.scr and sets following the registry entry with the path to this copy:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ExeName32

W32/Scold-A sends itself to all entries from the Outlook Address Book and in addition searches for e-mail addresses in HTM and HTML files from the IE Save folder and CTT files from the MY Documents folder.

W32/Yaha-Y (Aliases: WORM_YAHA.AF, W32/Yaha.y@MM, W32.Yaha.AF@mm) (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads by copying itself to network shares and by e-mailing itself to addresses found within files and registry entries on the local computer. The e-mail subject line, message text and attachment filename are randomly selected from internal lists. When first run, the worm copies itself to the Windows System folder as EXE32.EXE and MSMGR32.EXE with the hidden attributes set and creates the following registry entries to run itself on startup:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MsManager =
<SYSTEM>\MSMGR32.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MsManager =
<SYSTEM>\MSMGR32.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\MsManager =
<SYSTEM>\MSMGR32.EXE

The worm also prepends <SYSTEM>\EXE32.EXE to the following registry entries, so that EXE32.EXE is run whenever any file with an extension of EXE, COM, BAT or SCR is run or opened:

- HKCU\batfile\shell\open\command
- HKCU\comfile\shell\open\command
- HKCU\exefile\shell\open\command
- HKCU\scrfile\shell\open\command

The files Hosts and Lmhosts are dropped to the Windows folder and MSS32.DLL is dropped to the System folder. W32/Yaha-Y copies itself as MSMGR32.EXE to StartUp folders on local and network drives. The worm also copies itself to the Windows folder of network shares as EXE32.EXE and adds a new line "run=EXE32.EXE" to the [Windows] section of <WINDOWS>\Win.ini to run EXE32.EXE on startup. While the worm is active it continually tries to terminate selected anti-virus and security related processes and resets the registry entries mentioned above if they are changed or deleted. The worm disables Regedit.exe by setting the registry entry:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools = 1

W32.Randex.BD (Win32 Worm): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from its author. The existence of the files CfgDll32.exe or cmst32.exe is an indication of a possible infection. It is written in Microsoft Visual C++ and is packed with UPX.

Worm/Agobot.215552 (Internet Worm): This is a memory resident Internet worm that spreads through open or weakly protected network shares. It also exploits some well-known Microsoft vulnerabilities in order to propagate itself. If executed, the worm adds the following file to the \windows%\system% directory, "mwincfg32.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Config Loader for Microsoft Windows"="mwincfg32.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices "Config Loader for Microsoft Windows"="mwincfg32.exe"

The follow registry key is also created:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CfgLoad32
"ImagePath"=hex(2):22,00,43,00,3a,00,5c,00,57,00,49,00,4e,00,44,00,4f,00,57,00,53,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,6d,00,77,00,69,00,6e,00,63,00,66,00,67,00,33,00,32,00,2e,00,65,00,78,00,65,00,22,00,20,00,2d,00,73,00,65,00,72,00,76,00,69,00,63,00,65,00,00,00

Worm/Agobot.231936 (Internet Worm): This is a memory resident Internet worm that spreads through open or weakly protected network shares. It also exploits some well-known Microsoft vulnerabilities in order to propagate itself. If executed, the worm adds the following file to the \windows%\system% directory, "wincomm.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Windows Communicator"="wincomm.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices "Windows Communicator"="wincomm.exe"

Worm/Agobot.214528 (Internet Worm): This is a memory resident Internet worm that spreads through open or weakly protected network shares. It also exploits some well-known Microsoft vulnerabilities in order to propagate itself. If executed, the worm adds the following file to the \windows%\system% directory, "cart322.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "ConfigLoader"="cart322.exe"

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
"ConfiggLoader"="cart322.exe"

The follow registry key is also created:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\A3
"ImagePath"=hex(2):22,00,43,00,3a,00,5c,00,57,00,49,00,4e,00,44,00,4f,00,57,00,53,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,63,00,61,00,72,00,74,00,33,00,32,00,32,00,2e,00,65,00,78,00,65,00,22,00,20,00,2d,00,73,00,65,00,72,00,76,00,69,00,63,00,65,00,00,00.

Worm/Agobot.68608 (Internet Worm): This is a memory resident Internet worm that spreads through open or weakly protected network shares. It also exploits some well-known Microsoft vulnerabilities in order to propagate itself. If executed, the worm adds the following file to the \windows%\system% directory, "scvhost.exe." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
""Configuration Loader"="scvhost.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
"Configuration Loader"="scvhost.exe"

Worm/Ardurk.G (Internet Worm): This is a memory resident Internet worm that spreads over e-mail. It copies itself over all shared folders. If executed, the worm adds the following file to the \windows%\system% directory, "I_LOVE_YOU.EXE.." The follow registry key is created:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i_love_you.exe
"ImagePath"=hex(2):43,00,3a,00,5c,00,57,00,49,00,4e,00,44,00,4f,00,57,00,53,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,69,00,5f,00,6c,00,6f,00,76,00,65,00,5f,00,79,00,6f,00,75,00,2e,00,65,00,78,00,65,00,00,00 "DisplayName"="i_love_you.exe"

WORM_RANDEX.BF (Aliases: W32/Randbot.worm, Win32.HLLW.Randex,

W32/Randex.BF.worm) (Win32 Worm): This worm spreads via network shares using a list of predefined passwords. It also has backdoor capabilities. It connects to an IRC (Internet Relay Chat) server and waits for commands from a remote user to process on the infected system. It allows remote users to scan through the infected system and retrieve information. This memory-resident worm runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_SDBOT.AZ (Aliases: Backdoor.SDBot.Gen, Backdoor/SdBot.Server,

IRC/BackDoor.SdBot.VW) (Win32 Worm): This worm drops a copy of itself using the file name, WUPDATED.EXE, in the Windows system folder. It then modifies the Windows registry so that it is executed at every system startup. It spreads through the network by dropping copies of itself in shared drives with read/write access. It either establishes a connection to the IPC\$ share, or it uses its own list of user names and passwords to log on to the system. The worm also propagates via the Internet, specifically through chat programs, by sending a copy of itself to all contacts found. This malware also carries a backdoor routine. It has a built in IRC (Internet Relay Chat) client engine, which enables it to connect to an IRC channel and await commands from a remote user. It runs on Windows NT, 2000 and XP.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
A97M/AcceV	N/A	CyberNotes-2003-18
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
Afcore.q	N/A	CyberNotes-2003-20
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	CyberNotes-2003-18
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Asoxy	N/A	CyberNotes-2003-24
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Augudor	N/A	CyberNotes-2003-23
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Beasty.Kit	N/A	CyberNotes-2003-18
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bionet.404	404	CyberNotes-2003-23
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Ciadoor.B	B	CyberNotes-2003-24
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Coreflood.dr	Dr	CyberNotes-2003-19
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.CrashCool	N/A	CyberNotes-2003-19
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Daemonize	N/A	CyberNotes-2003-21
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Defcode	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Dister	N/A	CyberNotes-2003-23
Backdoor.DMSpammer	N/A	CyberNotes-2003-22
Backdoor.Dragonqq	N/A	Current Issue
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Evilbot.B	B	CyberNotes-2003-19
Backdoor.Evilbot.C	C	CyberNotes-2003-22
Backdoor.EZBot	N/A	CyberNotes-2003-18
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.Formador	N/A	Current Issue
Backdoor.Frango	N/A	CyberNotes-2003-22
Backdoor.Freefors	N/A	Current Issue
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Graybird.G	G	CyberNotes-2003-19
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Haxdoor	N/A	Current Issue
Backdoor.Hazzer	N/A	CyberNotes-2003-20
Backdoor.Helios.B	B	CyberNotes-2003-23
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hogle	N/A	CyberNotes-2003-22
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	CyberNotes-2003-18
Backdoor.IRC.Bot.B	B	CyberNotes-2003-22
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	CyberNotes-2003-18
Backdoor.IRC.Jemput	N/A	CyberNotes-2003-19
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	CyberNotes-2003-18
Backdoor.IRC.RPCBot.C	C	CyberNotes-2003-18
Backdoor.IRC.RPCBot.D	D	CyberNotes-2003-18
Backdoor.IRC.RPCBot.F	F	CyberNotes-2003-19
Backdoor.IRC.Tastyred	N/A	CyberNotes-2003-20
Backdoor.IRC.Whisper	N/A	CyberNotes-2003-24
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Yoink.A	A	CyberNotes-2003-23
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.IRC.Zcrew.B	B	CyberNotes-2003-19
Backdoor.Isen.Rootkit	N/A	CyberNotes-2003-23
Backdoor.Jittar	N/A	CyberNotes-2003-21
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Ketch	N/A	Current Issue
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lassrv	N/A	CyberNotes-2003-21
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Lixy	N/A	CyberNotes-2003-21
Backdoor.Lixy.B	B	CyberNotes-2003-22
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	N/A	CyberNotes-2003-17
Backdoor.Madfind	N/A	CyberNotes-2003-23
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MeteorShell	N/A	CyberNotes-2003-21
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
Backdoor.Mprox	N/A	CyberNotes-2003-20
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Mxsender	N/A	CyberNotes-2003-21
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Omygo	N/A	CyberNotes-2003-19
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peeper	N/A	CyberNotes-2003-20
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Pspider.310.b	310.b	CyberNotes-2003-18
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Rado	N/A	CyberNotes-2003-18
Backdoor.Ranck	N/A	CyberNotes-2003-18
Backdoor.Ranck.C	C	CyberNotes-2003-22
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remocy	N/A	CyberNotes-2003-22
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.Roxy.B	B	CyberNotes-2003-20
Backdoor.RPCBot.E	E	CyberNotes-2003-19
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	P	CyberNotes-2003-17
Backdoor.SDBot.Q	Q	CyberNotes-2003-21
Backdoor.Sdbot.R	R	CyberNotes-2003-21
Backdoor.Semes	N/A	CyberNotes-2003-20
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sheldor	N/A	CyberNotes-2003-18
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sincom	N/A	CyberNotes-2003-21
Backdoor.Sinit	N/A	CyberNotes-2003-21
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Smokodoor	N/A	CyberNotes-2003-21
Backdoor.Smother	N/A	CyberNotes-2003-20
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Sokacaps	N/A	CyberNotes-2003-18
Backdoor.Spotcom	N/A	CyberNotes-2003-24
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.Surdux	N/A	CyberNotes-2003-20
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Tinydog	N/A	CyberNotes-2003-24
Backdoor.Translat	N/A	CyberNotes-2003-20
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Urat.b	b	CyberNotes-2003-18
Backdoor.Usirf	N/A	CyberNotes-2003-21
Backdoor.Uzbet	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wollf.16	16	CyberNotes-2003-18

Trojan	Version	CyberNotes Issue #
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.Xibo	N/A	Current Issue
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zinx	N/A	CyberNotes-2003-23
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zombam.B	B	CyberNotes-2003-20
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-ATM.gen	N/A	CyberNotes-2003-24
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
Backdoor-AZF	AZF	CyberNotes-2003-20
BackDoor-BAE	BAE	CyberNotes-2003-21
BackDoor-BBO	BBO	CyberNotes-2003-22
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Carufax.a	A	Current Issue
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/IRCBot.13856	13856	Current Issue
BDS/IRCBot.82779	82779	CyberNotes-2003-23
BDS/PowerSpider.A	A	CyberNotes-2003-11
BDS/Purisca	N/A	Current Issue
BDS/SdBot.76870	76870	CyberNotes-2003-21

Trojan	Version	CyberNotes Issue #
BDS/Spyboter	N/A	Current Issue
BKDR_LITH.103.A	A	CyberNotes-2003-17
Cardown	N/A	CyberNotes-2003-19
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
Delude	N/A	CyberNotes-2003-19
Desex	N/A	CyberNotes-2003-20
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	CyberNotes-2003-18
Download.Magicon	N/A	CyberNotes-2003-22
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Dluca.B	B	CyberNotes-2003-19
Downloader.Dluca.C	C	CyberNotes-2003-20
Downloader.Dluca.D	D	CyberNotes-2003-22
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader.Slime	N/A	CyberNotes-2003-21
Downloader.Tooncom	N/A	CyberNotes-2003-22
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-BW.h	BW.h	CyberNotes-2003-23
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	CyberNotes-2003-18
DownLoader-EG	EG	CyberNotes-2003-20
Downloader-ES	ES	CyberNotes-2003-22
Downloader-EU	EU	CyberNotes-2003-22
Downloader-EV	EV	CyberNotes-2003-22
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Enocider	N/A	CyberNotes-2003-22
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.Keystel	N/A	CyberNotes-2003-19
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IgetNet.dr	dr	CyberNotes-2003-21
IRC.Trojan.Fgt	Fgt	CyberNotes-2003-22
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Fortnight.D	D	CyberNotes-2003-22
JS.Pun.Trojan	N/A	Current Issue
JS.Seeker.J	J	CyberNotes-2003-01
JS.Seeker.K	K	CyberNotes-2003-20
JS/AdClicker-AB	AB	Current Issue
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Mico	N/A	CyberNotes-2003-20
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MouseLog-Ladora	N/A	CyberNotes-2003-22
MultiDropper-FD	N/A	CyberNotes-2003-01
OF97/ExeDrop-B	N/A	CyberNotes-2003-19
Pac	N/A	CyberNotes-2003-04
Petala	N/A	CyberNotes-2003-20
PHP.Rumaz.Trojan	N/A	CyberNotes-2003-23
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
Proxy-Regate	N/A	CyberNotes-2003-22
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Bugmaf	N/A	CyberNotes-2003-21

Trojan	Version	CyberNotes Issue #
PWS-Mob	N/A	CyberNotes-2003-22
PWS-Moneykeeper	N/A	CyberNotes-2003-18
PWS-Sincom.dr	dr	CyberNotes-2003-17
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.ALlight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Bancos.C	C	CyberNotes-2003-22
PWSteal.Banpaes	N/A	CyberNotes-2003-21
PWSteal.Banpaes.B	B	CyberNotes-2003-24
PWSteal.Finero	N/A	CyberNotes-2003-21
PWSteal.Firum	N/A	CyberNotes-2003-22
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Ldpinch	N/A	CyberNotes-2003-23
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	CyberNotes-2003-18
PWSteal.Lemir.E	E	CyberNotes-2003-20
PWSteal.Lemir.F	F	CyberNotes-2003-20
PWSteal.Nikana	N/A	CyberNotes-2003-21
PWSteal.Reanet	N/A	CyberNotes-2003-21
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Salira	N/A	CyberNotes-2003-21
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWSteal.Tarno	N/A	CyberNotes-2003-22
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	N/A	CyberNotes-2003-17
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial15	15	CyberNotes-2003-22
QDial6	6	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-AD.dr	AD.dr	Current Issue
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
StartPage-U	U	CyberNotes-2003-20
StartPage-W	W	CyberNotes-2003-22
Stash	N/A	CyberNotes-2003-23
Stealthier	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Apdoor-A	A	CyberNotes-2003-19
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Backsm-A	A	CyberNotes-2003-19
Troj/Bdoor-AAG	AAG	CyberNotes-2003-21
Troj/Bdoor-RQ	RQ	CyberNotes-2003-17
Troj/CoreFloo-C	C	CyberNotes-2003-22
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/Dloader-F	F	Current Issue
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Eyeveg-A	A	CyberNotes-2003-19
Troj/Golon-A	A	CyberNotes-2003-15
Troj/HacDef-084	N/A	CyberNotes-2003-24
Troj/Hackarmy-A	A	CyberNotes-2003-20
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Ircbot-M	M	CyberNotes-2003-21
Troj/IRCBot-P	P	CyberNotes-2003-22
Troj/Litmus-AS	AS	CyberNotes-2003-24
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qhosts-1	N/A	CyberNotes-2003-20
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/Sysbug-A	A	CyberNotes-2003-24
Troj/TKBot-A	A	CyberNotes-2003-04
Troj/Tofger-A	A	CyberNotes-2003-24
Troj/Webber-A	A	CyberNotes-2003-15
Troj/Webber-C	C	CyberNotes-2003-23
Troj/Zana-A	A	Current Issue
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_MSNMASMSG.A	A	Current Issue
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Abaxo	N/A	CyberNotes-2003-20
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	N/A	CyberNotes-2003-17
Trojan.Androv	N/A	CyberNotes-2003-23
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Bedrill	N/A	CyberNotes-2003-23
Trojan.Benuti	N/A	Current Issue
Trojan.Bootconf	N/A	CyberNotes-2003-21
Trojan.Boxer	N/A	CyberNotes-2003-19
Trojan.Cuydoc	N/A	CyberNotes-2003-21
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Digits	N/A	Current Issue
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Framar	N/A	Current Issue
Trojan.Fwin	N/A	CyberNotes-2003-18
Trojan.Gaslide.Intd	N/A	CyberNotes-2003-20
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.Kalshi	N/A	CyberNotes-2003-21
Trojan.KillAV.B	B	CyberNotes-2003-19
Trojan.KillAV.C	C	CyberNotes-2003-23
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Loome	N/A	CyberNotes-2003-22
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Mumuboy.B	B	CyberNotes-2003-20
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Myss.B	B	CyberNotes-2003-21
Trojan.Naldem	N/A	CyberNotes-2003-23

Trojan	Version	CyberNotes Issue #
Trojan.Norio	N/A	CyberNotes-2003-19
Trojan.Obsorb	N/A	CyberNotes-2003-22
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.PWS.QQPass.E	E	CyberNotes-2003-20
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Retsam	N/A	CyberNotes-2003-22
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Sinkin	N/A	CyberNotes-2003-21
Trojan.Slog	N/A	Current Issue
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Vardo	N/A	CyberNotes-2003-20
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
Trojan.Gaslid	N/A	CyberNotes-2003-18
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.Bootconf	N/A	CyberNotes-2003-23
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	N/A	CyberNotes-2003-17
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.Noex.Trojan	N/A	CyberNotes-2003-23
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS.Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Adclicker.G.Trojan	G	CyberNotes-2003-22
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Hostidel.Trojan	N/A	CyberNotes-2003-24
W32.Hostidel.Trojan.B	B	CyberNotes-2003-24
W32.Laorenshe.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09

Trojan	Version	CyberNotes Issue #
W32.Petch.B	B	CyberNotes-2003-23
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Tofazzol	N/A	CyberNotes-2003-22
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32.Igloo-15	N/A	CyberNotes-2003-04
W97M.Tabi.Trojan	N/A	CyberNotes-2003-20
Woodcot	N/A	CyberNotes-2003-16
X97M.Sysbin	N/A	CyberNotes-2003-22
Xin	N/A	CyberNotes-2003-03

Backdoor.Dragonqq (Alias: PWS-QQDrag): This is a Trojan Horse that attempts to steal passwords from a Chinese instant messaging program and gives unauthorized access to a malicious user. This threat is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required to execute Backdoor.Dragonqq.

Backdoor.Formador (Aliases: Backdoor.Trojan.Client, Backdoor.Formador.c, Downloader-DP):

This is a Backdoor Trojan Horse that allows a malicious user to control your computer. When Backdoor.Formador is copied to the %System% folder and executed, it adds the value, <executed file name>="%System%\<execute file name>.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the backdoor runs when you start Windows. The Trojan requests a set of commands from a predetermined Web site.

Backdoor.Freefors: This is a Backdoor Trojan Horse that gives a malicious user unauthorized access to an infected computer. It is written in Microsoft Visual C++ and is packed with UPX. When Backdoor.Freefors is executed, it copies itself as %Windir%\msmq.exe and adds the value, "Message Queuing"="%Windir%\msmq.exe /nodelay /fastlogon /synclinks," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. The Trojan also adds the values:

- "DsValidSma0"="<Random Binary>"
- "DsValidRates"="<Random Binary>"
- "DsValidCerts"="<Random Binary>"

to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters

It attempts to download a file from a predetermined Web site to verify whether the Trojan is the latest version. If it is not, it will update itself to the latest version.

Backdoor.Haxdoor (Alias: Backdoor.Haxdoor.i): This is a Backdoor Trojan Horse that opens TCP ports, allowing unauthorized access to an infected computer. When Backdoor.Hoxdoor runs, it copies itself as %System%\JSDAPI.EXE and registers and runs JSDAPI.EXE as a process. Backdoor.Haxdoor creates the following files to the %System% folder:

- DEBUGG.DLL
- BOOT32.SYS
- C3.DLL
- C3.SYS
- C4.SYS
- SMTAPI.SYS

And adds the following key to the system registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\debugg

which ensures that the Trojan runs when Windows NT is started. The Trojan also adds the subkey:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MPRServices\TestService\MPRServices\TestServices

which ensures that it runs when Windows is started.

Backdoor.Ketch: This is a backdoor Trojan Horse that allows a malicious user to control your computer by executing commands from a predetermined Web site. When Backdoor.Ketch is executed, it adds the value, "scheck"="%System%\scheck##.exe" (where ## represents a number), to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the backdoor runs when you start Windows. The Trojan creates a registry key:

- HKEY_LOCAL_MACHINE\Software\scheck

This key is used to store configuration information for the Trojan. It may create the following nonmalicious files in the %Windir% folder:

- scheck.dat
- scheck.tmp

Backdoor.Xibo (Alias: Backdoor.XLBH.b): This is a Backdoor Trojan Horse that opens TCP ports, allowing unauthorized access to an infected computer. When Backdoor.Xibo runs, it copies itself as %System%\services.exe and adds a service named "Services," and sets it to run the services.exe file. The following keys are added to the system registry:

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\servicese
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\servicese

BDS/Carufax.a (Alias: W32/Lazi@mm): Like other backdoors, BDS/Carufax.a would potentially allow someone with malicious intent remote access to your computer. If executed, the backdoor copies itself to the \windows%\system% directory as "INTERNT.EXE." It also adds the file "C:\WINDOWS\SYSTEM\KBDEXT32.DLL." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
"internt"="C:\\WINDOWS\\SYSTEM\\INTERNT.EXE"

BDS/IRCBot.13856: Like other memory resident backdoors, BDS/IRCBot.13856 would potentially allow someone with malicious intent remote access to your computer. If executed, the backdoor copies itself to the \windows%\system% directory as "sysweb.exe," So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"Setting"="sysweb.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"Setting"="sysweb.exe"

BDS/Purisca: Like other backdoors, BDS/Purisca remains memory resident and could potentially allow someone with malicious intent remote access to your computer. If executed, the backdoor copies itself in the \windows%\system% directory under the filename "winservn.exe." It will also copy itself at "C:\Program Files\PurityScan\PuritySCAN.exe." The file "C:\Documents and Settings\Makrorechner\Application Data\ewat.exe" then gets added. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
"Mtptr"="C:\\Documents and Settings\\Makrorechner\\Application Data\\ewat.exe"
"ContentService"="C:\\WINDOWS\\System32\\winservn.exe"

BDS/Purisca attempts to open an Internet Explorer window.

BDS/Spyboter: Like other memory resident backdoors, BDS/Spyboter would potentially allow someone with malicious intent remote access to your computer. If executed, the backdoor copies itself to the

\windows\%system% directory as "SVCHOSTS.EXE." So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
"MicrosoftOutlook"="SVCHOSTS.EXE"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
"MicrosoftOutlook"="SVCHOSTS.EXE"

It also will modify the file C:\Windows\system.ini:

- C:\WINDOWS\system.ini
shell=explorer.exe SVCHOSTS.EXE
shell=explorer.exe

JS/AdClicker-AB: This threat is normally found named as HT.HTA. When the Trojan is executed, it will delete c:\HT.HTA if it exists. It will open up a series of advertisements that are mainly for porn sites.

JS.Pun.Trojan: This Trojan executes on startup and attempts to open two Web pages in Internet Explorer. When JS.Pun.Trojan runs, it copies itself as %Windir%\MSObject32.js and adds the value, "MSObject32"="%WinDir%\MSObject32.js," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

StartPage-AD.dr : This Trojan simply drops an executable into the Windows Startup folder (named start.exe), which alters the default start and search pages for Microsoft Internet Explorer each time your computer starts. The following registry entries are made:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Counter" = %incremental number%
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Search Bar" = <http://www.secret-crush.com/search/search.php>
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Use Custom Search URL" = 1
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchUrl "Search Page" = <http://www.secret-crush.com/%s>
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Search Page" = <http://www.secret-crush.com/search/search.php>
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Start Page" = <http://www.secret-crush.com/search/>
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search "CustomizeSearch" = <http://www.secret-crush.com/search/search.php>
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search "SearchAssistant" = <http://www.secret-crush.com/search/search.php>

Troj/Dloader-F: This Trojan has been reported in the wild. It attempts to download and execute an EXE file from the Internet. The Trojan attempts to download NEHER.GIF from bancoline.hotmail.ru, save it as HANGUP.EXE within the Windows folder and execute it. The file NEHER.GIF did not exist at the time of writing. The Trojan is configurable so filenames and URLs may change in the future.

Troj/Zana-A: This is a small browser application that displays material containing pornographic content. Additionally the website contacted by the Trojan may attempt to download a premium rate porn dialler.

Trojan.Benuti: This is a Trojan Horse that directly inserts mail into your Microsoft Outlook Inbox. It may also be used to distribute spam. When Trojan.Benuti is executed, it attempts to download data from a predetermined Web server and uses MAPI calls to save a new message into the current user's Outlook Inbox. The Trojan may create the following nonviral files in the %System% folder:

- mspr.dat
- winm.tmp

and may also add a value to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
so that the Trojan runs when you start Windows.

Trojan.Digits: This is a Trojan horse that modifies the Hosts file. It will also change your Internet Explorer home page and search pages to connect to a predetermined Web site.

Trojan.Framar: This is a Trojan Horse that terminates various process and opens TCP port 23435. It is packed with FSG. When Trojan.Framar is executed, it copies itself as %Windir%\Avsynmgr32e.exe and adds the value, "MSMcAfee"="%Windir%\Avsynmgr32e.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
so that the Trojan runs when you start Windows.

TROJ_MSNMASMSG.A (Aliases: Trojan.Win32.MSNFlood.28672, Flooder.MSN.VB.ac, Flooder:Win32/MSN.VB.AC, FDoS-MassMsg): This non-memory resident Trojan may arrive on a target system as the file WIN.SCR. It contains no propagation routine and needs to be run manually. It sends the message "win" via the IM Message window popup to all entries found in the Windows or MSN Messenger contact list of a target user. This Trojan has been tested to successfully send an IM message on Windows 2000. On Windows XP, however, it fails to perform its intended function due to programming errors. It is written in Visual Basic and runs on Windows 95, 98, ME, NT, 2000, and XP.

Trojan.Slog: This is a heavily encrypted Trojan Horse that changes Internet Explorer settings, and sends information about the host system to a remote server. Upon execution, Trojan.Slog modifies the following registry keys, changing the Internet Explorer Home page and Search pages:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Search Page
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Search Bar
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Use Search Assistant
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Default_Search_URL
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchURL
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Search\SearchAssistant

It attempts to contact out.true-counter.com and send system information about the infected computer to it. The Trojan adds the line, "645238813 auto.search.msn.com," to the file %System%\drivers\etc\hosts.